We claim:

Sub a'

1. A method for generating a configuration file for at least one firewall in a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets;

receiving an assignment of said roles to said hosts in said network; and

generating rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

2. The method of claim 1, wherein a configuration file is generated for a plurality of firewalls in said network.

3. The method of claim 1, wherein a security policy for said network is expressed in terms of said roles defining network capabilities of sending and receiving services.

4. The method of claim 1, wherein a plurality of said roles are combined into role-groups that may be assigned to one or more hosts.

5. The method of claim 1, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or a role-group.

6. The method of claim 1, further comprising the step of providing a visual representation of the structure of said hosts in said network.

7. The method of claim 1, further comprising the step of providing a visual representation of a set of rules in said configuration file.

8. The method of claim 1, wherein said generating step is performed by a vendor-specific compiler that produces a vendor-specific firewall configuration file.

9. A method for generating a configuration file for at least one firewall in a network, said network including a plurality of interconnected hosts, said method comprising the steps of:

utilizing a model definition language to produce an entity relationship model representing a security policy for said network; and

translating said entity relationship model into said firewall configuration file.

10. The method of claim 9, wherein a configuration file is generated for a plurality of firewalls in said network.

11. The method of claim 9, wherein said security policy is expressed in terms of roles that define network capabilities of sending and receiving services.

12. The method of claim 11, wherein said roles are assigned to said hosts.

13. The method of claim 11, wherein a plurality of said roles are combined into role-groups that may be assigned to a host.

14. The method of claim 11, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or a role-group.

15. The method of claim 9, further comprising the step of providing a visual representation of the structure of said hosts in said network.

16. The method of claim 9, further comprising the step of providing a visual representation of a set of rules in said configuration file.

17. The method of claim 9, wherein a vendor-specific compiler translates said entity-relationship model into a vendor-specific firewall configuration file.

18. A method of producing an entity-relationship model representing the security policy for a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for one or more role entities that further define allowed services and a direction in which a service can be executed;

receiving a model of a topology of said network that partitions said network into one or more zones, connected by means of one or more gateways, each of said gateways having a gateway-interface for each adjacent zone;

receiving an assignment of said hosts to one or more zones; and

generating said entity-relationship model from said received definitions, model and assignments.

19. The method of claim 18, further comprising the step of assigning said roles to said hosts.

20. The method of claim 18, further comprising the step of defining one or more role-group entities consisting of a set of said role entities.

21. The method of claim 18, further comprising the step of translating said entity relationship model into a firewall configuration file.

22. The method of claim 21, wherein said configuration file is are generated for a plurality of firewalls in said network.

23. The method of claim 18, wherein said security policy is expressed in terms of roles that define network capabilities of sending and receiving services.

24. The method of claim 18, wherein a plurality of said role entities are combined into a role-group that may be assigned to a host.

25. The method of claim 18, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or a role-group entity.

26. The method of claim 18, further comprising the step of providing a visual representation of the structure of said hosts in said network.

27. The method of claim 21, further comprising the step of providing a visual representation of a set of rules in said configuration files.

28. The method of claim 18, wherein a vendor-specific compiler translates said entity-relationship model into vendor-specific firewall configuration files.

29. A method of generating a security policy for a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets;

receiving an assignment of said roles to said hosts in said network; and

generating said security policy from said received definitions and assignments.

30. The method of claim 29, further comprising the step of translating said security policy into at least one configuration file for a firewall on said network.

31. The method of claim 30, wherein said configuration files are generated for a plurality of firewalls in said network.

32. The method of claim 29, wherein a plurality of said roles are combined into a role-group that may be assigned to a host.

33. The method of claim 29, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or role-groups.

34. The method of claim 29, further comprising the step of providing a visual representation of the structure of said hosts in said network.

35. A compiler for generating a configuration file for a firewall in a network, said network including a plurality of hosts, comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets;

receive an assignment of said roles to said hosts in said network; and

generate rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

36. A firewall manager for generating a configuration file for a firewall in a network, said network including a plurality of interconnected hosts, comprising:

a parser utilizing a model definition language to produce an entity relationship model representing a security policy for said network; and

a compiler for translating said entity relationship model into said firewall configuration file.

37. A parser for producing an entity-relationship model representing the security policy for a network, said network including a plurality of hosts, said parser comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for one or more role entities that further define allowed services and a direction in which a service can be executed;

receive a model of a topology of said network by partitioning said network into one or more zones, connected by means of one or more gateways, ~~each of~~ said gateways having a gateway-interface for each adjacent zone;

receive an assignment of said hosts to one or more zones; and

generate said entity-relationship model from said received definitions, model and assignments.

38. A system for generating a security policy for a network, said network including a plurality of hosts, said system comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets;

receive an assignment of roles to said hosts in said network; and

generate said security policy from said received definitions and assignments.